Whitepaper

Increased targeting of mobile devices: **How to Protect Company Smartphones**

ESET® Digital Security
Progress. Protected.

Publication date:
10. 30. 2024

Table of Contents

Introduction

In a contemporary business landscape, integrating smartphones at the workplace is no longer a novelty but a necessity. These versatile devices have become indispensable tools for communication, task management, access to information and even control of business processes in real time. Their ability to store and process sensitive data, combined with their portability, provides unprecedented flexibility which allows employees to work from anywhere, anytime.

However, this convenience comes with increased data security risks. Enterprise smartphones are often home to critical data such as customer personal information, financial data, trade secrets and internal correspondence. This concentration of sensitive information, along with the connected nature of smartphones, makes them prime targets for cyberattacks. Phishing, malware, denial of service attacks and spying are all threats that enterprises must now consider as daily risks. Faced with this realization, implementing robust cybersecurity solutions that are adapted to the specifications of smartphones is essential.

Protecting traditional IT infrastructures is no longer sufficient; instead, we must extend security to devices that travel well beyond the company's physical boundaries. This includes implementing strict security policies, installing advanced security software, training employees on cybersecurity best practices and creating incident response plans.

The final objective of these measures is twofold: to preserve the confidentiality, integrity and availability of enterprise data while maintaining the productivity and flexibility that smartphones provide. In this whitepaper, we will explore the challenges and solutions associated with securing smartphones in an enterprise environment in more detail, with the objective of providing a framework for navigating this complex and rapidly evolving landscape.

> "The device in your pocket can do much more than call or send messages. **Your smartphone stores almost every aspect of your life,** from memories captured in photos to personal noties and scehdules, connection details and various other types of sensitive data."
>
> **Lukas Stefano**
> **Malware Researcher at ESET**

Chapter 1: General use of smartphones at the workplace

Smartphones at the workplace have undergone significant changes in recent years, transforming the way organizations operate and interact both internally and with their customers and partners. Here is a detailed overview of how smartphones are used in a business setting.

- **REMOTE WORK**
  The COVID-19 pandemic accelerated the transition to remote work, making smartphones even more essential to remote employees. These devices allow you to stay connected with other employees, access online resources, collaborate on documents and maintain productivity outside of the traditional office environment.

- **BUSINESS / PERSONAL USAGE**
  With the increase of working remotely, enterprise smartphones are frequently used for unplanned personal activities, such as social media and personal applications, in addition to their business functions like emails and virtual meetings. This inappropriate practice of combining uses raises important security questions, in particular separating business and personal data.

- **BYOD**
  The BYOD (Bring Your Own Device) concept allows employees to use their personal devices, such as smartphones, for business tasks. The COVID-19 pandemic has prompted 85%* of organizations to implement BYOD policies. This approach provides increased flexibility and can improve employee satisfaction because it allows them to use devices they already feel comfortable with. However, BYOD also presents data security challenges because it is difficult to control how personal devices are used and secured.

48% of enterprises choosing BYOD today say they have seen malware introduced by an employee's personal phone, and only 4 out of 10 have used Mobile Device Management (MDM).[1]

66% 66% of workers who depend on technology use smartphones.[2]

[1] 2023 Samsung Survey / [2] Verizon, "2023 Data Breach Investigations Report"

Chapter 2: Evolution of threats on smartphones

The constantly evolving world of mobile technologies is unfortunately accompanied by a parallel increase in cyber threats targeting these devices. Smartphones, which have become central to an enterprise's daily operations, are not immune to this worrying trend. This chapter explores the evolution of mobile cyberattacks, highlighting current trends and providing recent figures to illustrate the scale of the problem.

Mobile Ransomware

Mobile Phishing

Malware Applications

Wireless Network Attacks

Zero-day Vulnerabilities

- **RANSOMWARE**
  Mobile malware, particularly ransomware, has evolved to become more sophisticated. These malware programs are designed to infiltrate smartphones, often through compromised applications or malicious links, and can encrypt device data to demand a ransom.

- **PHISHING**
  Phishing, a well-known technique on computers, has been adapted in the mobile world. Attackers use SMS (smishing), emails or messaging applications to trick users into disclosing sensitive information or downloading malware.

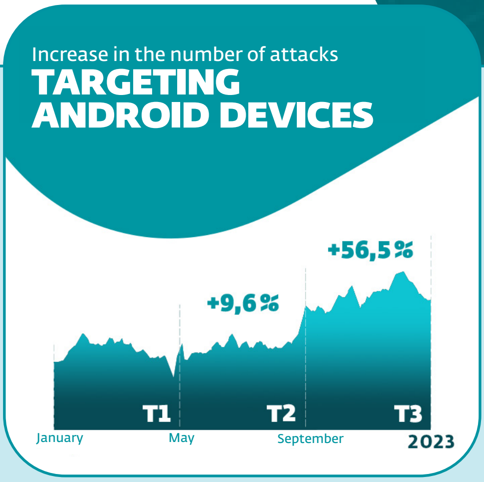
- **MALWARE APPLICATIONS**
  The number of malicious applications available on official and unofficial platforms continues to increase. These applications may appear legitimate but hide malicious features, ranging from data theft to signing up for paid services without user consent.

- **WIRELESS NETWORK ATTACKS**
  The number of malicious applications available on official and unofficial platforms continues to increase. These applications may appear legitimate

- **VULNERABILITIES**
  Zero-day vulnerabilities, for which there is no patch yet, are particularly popular with cybercriminals. These flaws can be exploited to take full control of a mobile device without the user realizing it.

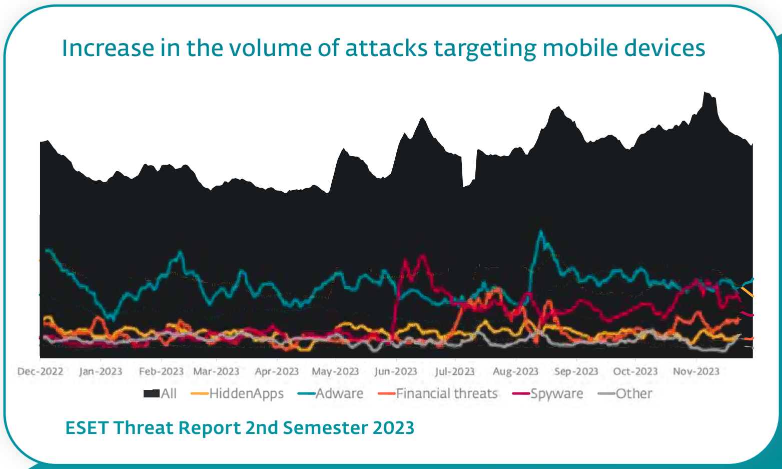
ATTACKS ON ANDROID ARE SHARPLY INCREASING

Attacks have increased in different sectors. Adware and hidden applications were the main types of malwares targeting Android devices. “Hidden malicious applications generally change their icon and hide on the device. They start displaying unwanted advertisements or performing other actions in the background,” explains Mr. Kubovic, Security Awareness Specialist at ESET.



Increase in the number of attacks
TARGETING ANDROID DEVICES

The volume of spyware is also increasing. “This type of malware is available on underground forums as a service allowing even unskilled attackers to buy and use it for a few hundred euros. Some have very extensive functions such as recording calls, taking control of the camera, stealing photos, emails and contacts,” explains Mr. Kubovic. Spyware generally aims to steal as much information and data as possible while secretly spying on the user. For attackers, this is a fairly easy way to make money, since the stolen data can be resold on the dark web and used in other attacks or for blackmail purposes.



Increase in the volume of attacks targeting mobile devices

ESET Threat Report 2nd Semester 2023

SMARTPHONES BECOME POPULAR TARGETS

While cybercriminals previously focused primarily on desktop devices and software, they are changing their focus since they understand that IT departments often have difficulty monitoring traffic and communications on mobile devices at the workplace.

“Smartphones tend to be undervalued, although crucial data can be stored on them, and they are used to access repositories and business applications. IT administrators often feel that the mobile environment is a little more secure due to compartmentalization and the fact that applications don’t have direct access to any activity of other applications on the device, but that’s not enough,” adds Mr. Kubovic.

However, cyber thieves can still find ways to gain access to the device, as in the case of the above threats.

“Financial mobile applications have been targeted recently, including those used for cryptocurrencies. This is likely because bitcoin and other cryptocurrencies are easier to launder or do not need to be laundered at all,” explains Mr. Kubovic, as one of the attackers’ motivations. “Mobile phones are our new wallets, and cybercriminals know it.”

In the past year, malware was downloaded onto the BYOD devices of 22% of enterprises. It is alarming that many enterprises do not know or cannot tell whether malware has been downloaded at the workplace.

[3]Bring-Your-Own-Device (BYOD) Market – Growth, Trends, Covid-19 Impact, and Forecasts (2021 – 2026)." by Mordor Intelligence

The evolution of cyber threats against mobile devices requires constant vigilance by enterprises and users. Recent figures illustrate not only the scale of the problem but also the need to adopt robust security measures, including extensive employee training, using advanced mobile security solutions and continuously updating systems and applications. Protecting against these evolving threats is essential to securing sensitive enterprise data and maintaining customer trust.

CONCRETE EXAMPLES

In 2021, ESET telemetry detected a 428% annual increase in banking malware with Android. The following year, the overall increase was driven by adware. In 2023, we saw a significant increase in Android spyware cases. Last year, ESET researchers discovered two active campaigns which targeted Android users spread across multiple application stores and dedicated websites.

Threatening actors patched the open-source Signal and Telegram applications for Android with malicious code that ESET researchers identified under the name BadBazaar. The malicious apps were named Signal Plus Messenger and FlyGram, and their aim was to exfiltrate user data such as contact lists, call logs and Google account lists.

Signal Plus Messenger is even more dangerous than FlyGram with its unique ability to spy on victim's communications in the original Signal application. This sensitive information could be used for other targeted phishing attacks against enterprise management.

A similar case was documented in June 2023, when ESET researchers identified an updated version of the Android spyware GravityRAT. It was distributed through malicious but functional messaging applications BingeChat and Chatico, which are both based on the OMEMO Instant Messenger application. This specific spyware can exfiltrate call logs, contact lists, SMS messages, device locations, basic device information and files with specific extensions, such as jpg, PNG, txt, pdf, etc.

And this is just the beginning. There are many ways in which smartphones can be attacked which can put an enterprise's finances and data at risk, such as through banking trojans, phishing, vulnerabilities or physical theft.

Chapter 3: Good practices: How to protect your fleet of smartphones

In a context where cyber threats to mobile devices are constantly evolving, ensuring the security of an enterprise's fleet of smartphones is becoming a major issue. Implementing proactive defense strategies is essential to protect sensitive data and preserve the integrity of information systems. Here is a series of recommended good practices to effectively secure mobile devices at the workplace.

> Integrating these practices into the enterprise's overall security strategy significantly minimizes the risks associated with the use of mobile terminals and reinforces the organization's position on cybersecurity.

- **REAL-TIME PROTECTION**

  Using security solutions that provide real-time protection against malware, phishing, and other cyberattacks is crucial. These tools continuously monitor suspicious activities, block intrusion attempts and warn users of potential threats. They are the first line of defense to detect and neutralize attacks before they access critical data.

- **MOBILE DEVICE MANAGEMENT (MDM)**

  Mobile Device Management (MDM) solutions allow centralized control of smartphones and tablets used in business settings. They facilitate implementing security policies, installing updates and secure applications remotely as well as deleting data remotely if the device is lost or stolen. MDM is an essential tool for maintaining security practices consistent across your fleet of smartphones.

- ## MULTI-FACTOR AUTHENTICATION (MFA)

  Multi-factor authentication (MFA) adds an extra layer of security when accessing enterprise applications and data, by requiring additional proof of identity beyond a simple password. This could include a temporary code sent through SMS, a phone call, or using an authenticator application on any defined device. MFA significantly reduces the risk of unauthorized access if login credentials are compromised.

- ## WI-FI NETWORK SECURITY

  Encourage the use of secure VPNs when connecting to public Wi-Fi networks to encrypt data traffic and protect against information being intercepted.

- ## TRAINING AND RAISING AWARENESS

  Training and raising employee awareness of the security risks associated with the use of smartphones at the workplace are essential. Regular sessions should be held to educate staff on security best practices, recognizing phishing attempts, and procedures to follow if an attack is suspected. Raising awareness is a critical component to reinforcing daily safety behavior.

- ## AUDIT AND PERIODIC SECURITY TESTS

  Periodically assessing mobile terminal security through audits and penetration testing helps identify and remediate vulnerabilities before they are exploited by attackers.

- ## STRICT SECURITY POLICIES

  Defining and applying strict security policies are fundamental to regulating the use of mobile terminals. This includes clear guidelines on the types of applications allowed, secure connection protocols, data storage and sharing and procedures if a device is lost or becomes compromised. These policies should be regularly reviewed and updated to adapt to the evolving threat landscape.

Chapter 4: ESET, ideal partner for your security

As you have understood, deploying real-time protection on mobile terminals and centralizing this protection on a unified cybersecurity platform is critically important. To protect this Achilles heel, we end this study with a chapter on what ESET, a major European player, is implementing to protect you.

Taking into consideration these threats, implementing a Mobile Device Management (MDM) policy represents a big step forward. For example, **ESET Mobile Threat Defense** provides administrators with the ability to monitor and control applications for Android and iOS. With endpoint protection included, **ESET Mobile Threat Defense** also provides anti-virus and anti-phishing functionality, giving enterprises more threat prevention capabilities against cyberattacks.

✓ **SECURITY**

Security features range from anti-malware, anti-phishing, anti-theft, device security to web access control and much more.

✓ **MANAGEMENT**

Management includes remotely wiping devices, restricting application installations, pre-configuring devices for users and other IT management related items.

✓ **MULTIPLE OS**

Mobile protection generally covers Android and Apple devices, the two most popular mobile operating systems. Since these systems are different, mobile protection capabilities may also vary.

✓ **SINGLE INTERFACE**

ESET Mobile Threat Defense is integrated with the ESET PROTECT platform, on-premise or in the Cloud. This makes centralizing the protection of all of these devices (PCs, mobile devices and servers) on a single management platform possible.

✓ **REMOTE DEPLOYMENT**

IT administrators can simply select the employees who need to protect their mobile terminals, and they will automatically receive a QR code to download ESET protection. Nothing is easier. Synchronization is transparent with cloud management platforms. ESET supports Microsoft Intune, Microsoft Entra ID, VMware Workspace ONE and Apple Business Manager.

✔ TWO-FACTOR AUTHENTICATION

ESET offers other security layers for your mobile devices. Two-factor authentication (2FA), for example, is an authentication method which verifies the identity of a user based on two distinct pieces of information. 2FA is much more powerful than traditional authentication with a password or static PIN. By complementing traditional authentication with a dynamic second factor, 2FA effectively reduces the risk of data breaches caused by weak or leaked passwords. ESET Secure Authentication is compatible with on-premise applications but also with operating system connections, VPNs, Remote Desktop, Web/Cloud services such as Microsoft ADFS 3.0, Office 365, Google Apps, Dropbox, Outlook Web Access, by offering a multitude of authentication methods.

✔ GOOGLE PLAY STORE

Since 2019, ESET has been a member of the App Defense Alliance and an active partner in the Malware Mitigation Program, which aims to quickly find potentially harmful apps and stop them before they become available on Google Play.

ESET has identified some of the most sophisticated threats targeting Android mobile devices in recent years. With this important partnership, ESET's research teams are closely involved in analyzing all applications and contributing to the protection of Google Play Store users.

This partnership goes a long way to powering ESET's powerful global telemetry. That's why we constantly update our products in order to confront recent threats.

> *"Our partnership with a respected member of the cybersecurity industry such as ESET strengthens protection of the Google Play ecosystem"*
>
> **Dave Kleidenmacher**
> Head of Android Security
> and Privacy at Google

At ESET, our vision does not stop at the workplace. We estimate that nowadays, a user has a PC and a smartphone at the workplace. This is why we extend our field of protection to the user.

The ESET Mobile Threat Defense module is completely free starting from the ESET PROTECT Advanced bundle (and all higher tier bundles). For each Endpoint license acquired, you have the option of securing a mobile, without any additional costs. In other words, a single license will allow all users to protect their computer and smartphone at the same time.

AI Native Prevention for Tomorrow's Threats

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

LEARN MORE

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

ESET®
Digital Security
Progress. Protected.